Claims

1. A method for evaluating a security risk of an application, said method comprising the steps of:

determining whether unauthorized access or loss of said data would cause substantial damage;

determining whether said application is vulnerable to attack by a third party;

determining whether the application is shared by different customers;

determining mitigation controls for the security risk of said application; and

assigning a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the determination in evaluating said security risk.

2. A method as set forth in claim 1 further comprising the step of determining whether said application is vulnerable to allow a third party unauthorized write access to data maintained by or accessed by said application.

3. A method as set forth in claim 1 further comprising the step of determining whether said application is subject to industry controls.

4. A method as set forth in claim 1 further comprising the step of determining whether said data is personal in nature.

5. A method as set forth in claim 1 further comprising the step of determining whether there is a known exploit for said application.

6. A method as set forth in claim 1 further comprising the step of determining whether an exploit for said application could be created.

7. A method as set forth in claim 1 further comprising the step of determining whether said application is vulnerable to allow a third party unauthorized read access to said data.

8. A method as set forth in claim 1 further comprising the steps of:

determining whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and

assigning a numerical value or weight corresponding to a significance of said security risk to the determination whether the vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs.

9. A method as set forth in claim 1 further comprising the step of determining whether data maintained by or accessed by said application is confidential.

10. A method as set forth in claim 1 further comprising the step of determining whether a customer has direct use of said application.

11. A method as set forth in claim 1 further comprising the step of determining whether said application is subject to industrial controls for security.

12. A method as set forth in claim 1 wherein said mitigation controls comprise an intrusion detection system.

13. A method as set forth in claim 1 wherein said mitigation controls comprise vulnerability scanning.

14. A method as set forth in claim 1 wherein said mitigation controls comprise health checking.

15. A method as set forth in claim 1 wherein said mitigation controls comprise a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems.

16. A method as set forth in claim 1 further comprising the step of considering an importance of a customer of said application in evaluating the security risk of said application.

17. A method as set forth in claim 1 further comprising the step of determining whether said application is vulnerable to allow a third party unauthorized administration authority.

18. A method as set forth in claim 1 further comprising the step of combining said numerical values or weights to evaluate said security risk.

19. A method as set forth in claim 1 further comprising the step of comparing said security risk to a cost savings provided by said application, and determining whether to certify said application for use based in part on said comparison.

20. A method as set forth in claim 1 further comprising the step of comparing said security risk to a revenue provided by said application, and determining whether to certify said application for use based in part on said comparison.

21. A computer program product for evaluating a security risk of an application, said computer program product comprising:

a computer readable medium;

first program instructions to receive user input as to whether unauthorized access or loss of said data would cause substantial damage, whether said application is vulnerable to attack by a third party, whether the application is shared by different customers, and mitigation controls for the security risk of said application; and

second program instructions to assign a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the determination in evaluating said security risk, and combine the numerical values or weights to evaluate the security risk; and wherein

said first and second program instructions are recorded on said medium.

22. A method for evaluating a security risk of an application, said method comprising the steps of:

determining whether unauthorized access or loss of data maintained or accessed by said application would cause substantial damage;

determining whether said application is shared by different customers;

determining whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and

assigning a numerical value or weight to each of the foregoing determinations, each of said numerical values corresponding to a significance of the determination in evaluating said security risk.

23. A method as set forth in claim 22 further comprising the step of combining the numerical values or weights to evaluate the security risk.

24. A computer program product for evaluating a security risk of an application, said computer program product comprising:

a computer readable medium;

first program instructions to receive user input as to whether unauthorized access or loss of data maintained or accessed by said application would cause substantial damage, whether said application is shared by different customers, and whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and

second program instructions to assign a numerical value or weight to each of the foregoing determinations, each of said numerical values corresponding to a significance of the determination in evaluating said security risk, and combine the numerical values or weight to evaluate the security risk; and wherein

said first and second program instructions are recorded on said medium.